UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,975	06/25/2001	Douglas D. Boom	219.40058X00	7054

26529 7590 11/24/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN/PDC
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/886,975	BOOM, DOUGLAS D.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,14-16,18,20,22-24,26 and 28* is/are rejected.

7)☐ Claim(s) *10-13,17,19,21,25,27 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are pending.

Claim Objections

2. Claims 10-13, 17, 19, 21, 25, 27, 29 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 14, 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Schuba et al., US patent 6,725,378.

In reference to claim 1:

Scuba et al. discloses a system for detecting and restricting denial of service attacks, comprising:

- A transmit algorithm to receive packets from a software application and discard packets that are determined to be from a zombie application, where the zombie application packets are discarded since the connection will be closed. (Column 8, lines 18-32)
- A receive algorithm to receive packets from a network interface and discard packets that are determined to be from a zombie application, where the packets received are refused since the connection is closed. (Column 8, lines 18-32)
- A monitor code in communications with the transmit algorithm and the receive algorithm to track the pattern of packet transmission and reception to and from the software application and determine that the software application is a zombie application based upon the pattern of packet transmission and reception. (Column 11, line 65 – Column 12, line 32)

In reference to claim 14:

Scuba et al. discloses a method of detecting and restricting denial of service attacks comprising:

- Monitoring incoming and outgoing packets to and from a software application, where the monitored packets are the monitored data streams. (Column 9, lines 15-32) (Column 5, lines 58 – Column 6, line 8)
- Placing said software application on a zombie list or a watch list when a pattern of the incoming or outgoing packets from the software application matches that of the characteristics of a zombie application, where the zombie list is the list

(Column 6, lines 30-37) from where the hosts have a rank. (Column 11, lines 8-15)

- Blocking reception and transmission of packets to the software application when the software application has been placed on the watch list or the zombie list in a previous cycle and the software application further exhibits the characteristics of a zombie application. (Column 11, line 65 – Column 12, line 32)

Claim 22 is rejected for the same reasons as claim 14.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-9, 15-16, 18, 20, 23-24, 26, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scuba et al. in view of Porras et al., US patent 6,321,338.

In reference to claim 2:

Scuba et al. fails to explicitly disclose the system recited in claim 1, wherein said monitor code determines that the software application is the zombie application by identifying that the software application is transmitting a large number of packets without

receiving any packets and placing the software application on a zombie list or a watch list.

Porras et al. (Column 13, lines 30-49) however, discloses a monitoring system wherein an application is determined to be bad by identifying that the software application is transmitting a large number of packets without receiving any packets and placing the software application on a zombie list or a watch list, where the large number of packets is transmitted without receiving packets when ratio of packets received to packets sent is unusually unbalanced.

Porras et al. (Column 2, lines 42-53) teaches that an advantage is provided with the monitoring system in that it protects the network from intrusion, as well as detecting abnormal activity without requiring an administrator to catalog each type of attack on the network, allowing for some protection even when attacks have not yet been described by an administrator.

It would have been obvious to one of ordinary skill in the art at the time of invention to use the software monitor of Porras et al. as the monitor of Schuba et al. in order to provide greater protection for attacks that an administrator has not yet cataloged.

Claim 3, 15, 20, 23, 28 is rejected for the same reasons as claim 2.

In reference to claim 4:

Scuba et al. fails to explicitly disclose the system recited in claim 1, wherein said monitor code determines that the software application is the zombie application by

identifying that the software application is not receiving any packets and placing the software application on a watch list.

Porras et al. (Column 6, lines 10-25) discloses a monitoring system where the application is bad by identifying that the software application is not receiving any packets and placing the software application on a watch list, where the software is "profiled" as an anomaly when an abnormal loss of received packets is detected.

Porras et al. (Column 2, lines 42-53) teaches that an advantage is provided with the monitoring system in that it protects the network from intrusion, as well as detecting abnormal activity without requiring an administrator to catalog each type of attack on the network, allowing for some protection even when attacks have not yet been described by an administrator.

It would have been obvious to one of ordinary skill in the art at the time of invention to use the software monitor of Porras et al. as the monitor of Schuba et al. in order to provide greater protection for attacks that an administrator has not yet cataloged.

In reference to claim 5:

Scuba et al. fails to explicitly disclose the system recited in claim 4, wherein said monitor code alerts the user and the transmit algorithm and receive algorithm that a software application is a zombie application when the software application has previously been placed on the watch list and the software application is now transmitting a large number of packets.

Porras et al. (Column 13, lines 60-65) discloses a monitoring system where the application is bad by identifying that the software application is not receiving any packets

and placing the software application on a watch list, where the traffic is marked as malicious traffic if the application was receiving little or few packets, and is now transmitting a large number of packets.

Porras et al. (Column 2, lines 42-53) teaches that an advantage is provided with the monitoring system in that it protects the network from intrusion, as well as detecting abnormal activity without requiring an administrator to catalog each type of attack on the network, allowing for some protection even when attacks have not yet been described by an administrator.

It would have been obvious to one of ordinary skill in the art at the time of invention to use the software monitor of Porras et al. as the monitor of Schuba et al. in order to provide greater protection for attacks that an administrator has not yet cataloged.

Claims 6,8, 16, 18, 24, 26 are rejected for the same reasons as claim 4.

Claims 7, 9 are rejected for the same reasons as claim 5.

Conclusion

7. The following art not relied upon is made of record.

- Joyce, US patent 6,519,703 discloses a method for processing and analyzing packets in a firewall and granting each stream a confidence rating.
- Scambray et al. "Hacking Exposed", October 18th 2000, 2nd Edition, pgs 499-501 discloses the DDOS zombie attacks and some methods well known in the art to prevent them.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (571)272-3535. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

November 16th, 2004

TMH

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100